Annals of Mathematics, 128 (1988), 1–18

On the ideal class groups of real abelian number fields*

By Francisco Thaine

Introduction

In this paper we show a relation between the ideal class groups and the groups of units of real abelian number fields. It is obtained by means of an extension of the method of Kummer that leads to Stickelberger's theorem but, unlike this theorem, the results are more naturally stated for real fields.

Let $K \neq \mathbf{Q}$ be a real abelian number field, ζ_m a primitive m-th root of unity where m is the least positive integer such that $K \subseteq \mathbf{Q}(\zeta_m)$. Let E be the group of units of the ring of integers of K, A the ideal class group of K and Δ the Galois group of $K/\mathbf{Q}$. For $j \geq 1$ we define the following sets of rational functions in the indeterminate X:

$$C_j(X) = \left\{ f(X) = \pm \prod_{i=1}^{j} \prod_{k=1}^{m-1} \left(X^i - \zeta_m^k\right)^{a_{ik}} : \right.$$
$$\left. a_{ik} \in \mathbf{Z},\ f(X) \in K(X) \text{ and } f(1) \in E \right\}.$$

Let $C = \bigcup_{j=1}^{\infty} C_j(1)$. Since E is a noetherian $\mathbf{Z}$-module, there exists $l \geq 1$ such that $C = C_l(1)$. It is a subgroup of finite index of E that we call the group of circular units. This set certainly contains the set of circular units defined by Sinnot in [11], but I do not know whether or not it is substantially larger.

Let $W = E/C$ and, for p prime, let $(A)_p$ and $(W)_p$ be the p-Sylow subgroups of A and W. Our principal aim is to obtain annihilators (in $\mathbf{Z}[\Delta]$) of $(A)_p$ from annihilators of $(W)_p$. The main result proved in the article (Theorem 3) is that if $p \nmid [K:\mathbf{Q}]$ and if $\theta \in \mathbf{Z}[\Delta]$ annihilates $(W)_p$, then 2θ annihilates $(A)_p$. It is due, in this complete form, to Washington and Rubin (see below).

In the first section we work in an extension $L = K(\zeta_q)$ where ζ_q is a q-th primitive root of unity and q is an odd rational prime, greater than l, that splits completely in K.

*This research was partially done at Queen's University and at the University of Maryland at College Park where the author held a fellowship of the Brazilian CNPq.

Let s be a primitive root modulo q and τ the generator of the Galois group of L/K such that $\tau(\zeta_q) = \zeta_q^s$. Given $f(X) \in C_l(X)$, the norm $N_{L/K}(f(\zeta_q))$ is equal to 1 (Proposition 1) so that, by Hilbert's Theorem 90, there exist non-zero elements α of L such that $\tau(\alpha) = f(\zeta_q)\alpha$.

We study the prime ideal factorization of the principal ideal (α) generated by one of such elements. It results that

$$\text{(i)} \qquad (\alpha) = D \prod_{\sigma \in \Delta} \sigma^{-1}(B)^{r_\sigma},$$

where D is the lift of an ideal of K, B is a prime ideal of L above q and where we denote by σ both the element of Δ and its extension to L that fixes ζ_q.

We also show that

$$\text{(ii)} \qquad s^{r_\sigma} \equiv \sigma(f(1)) \bmod Q, \quad \text{for all } \sigma \in \Delta,$$

where $Q = B \cap K$ (Proposition 2). This determines the exponents r_σ modulo $q - 1$.

It has been pointed out by Washington that the principal ideas of this section were already developed by Kummer in [5], and that in fact it seems to be the first time in which Hilbert's Theorem 90 (which is due to Kummer) appears and is applied.

In the second section we relate the factorization of the elements α mentioned above with the structure of the units of K. To induce an order in K we fix an embedding of K into $\mathbf{R}$ and define $|x| = \sup\{x, -x\}$ if $x \in K$.

Let $\delta \in C \setminus \{\pm 1\}$, $\delta = f(1)$ with $f(X) \in C_l(X)$. For each prime ideal Q of K above an odd rational prime $q > l$ splitting completely in K, let $s = s_Q$ be a primitive root modulo q and $r_\sigma = r_\sigma(Q)$ as in (ii). Given an ideal class $\mathscr{C} \in A$ and a positive integer b, we define $P(\mathscr{C}, b)$ as the set of all prime ideals $Q \in \mathscr{C}$, above odd rational primes $q > l$ splitting completely in K and such that $q \equiv 1 \bmod b$. If $P(\mathscr{C}, b)$ is non-empty and $\sigma \in \Delta$ let g be the greatest common divisor of b and of all the $r_\sigma(Q)$ such that $Q \in P(\mathscr{C}, b)$. Given $\varepsilon \in E$, $\varepsilon \neq \pm 1$, we define $\phi(\varepsilon)$ as the greatest integer k such that $\varepsilon = \mu^k$ for some $\mu \in K$. Denote by (a, b) the greatest common divisor of the integers a and b. We prove (Theorem 1) that when $P(\mathscr{C}, b)$ is non-empty, $g = (\phi(\delta), b)$ if b is odd, $g = (\phi(\delta), b)$ or $g = 2(\phi(\delta), b)$ if b is even and $\sigma(\delta) > 0$, and g divides $(4/(2, b/g))(\phi(|\delta|), b)$ and is divided by $(\phi(\delta), b)$ in any case.

The result above is based on a local-global theorem (Proposition 4(d)) which proof depends on the Tchebotarev Density Theorem. The help given and the beautiful theorems of class field theory shown to me by Lawrence Washington and René Schoof were essential to get this theorem. The strategy of the proof was suggested by Washington and the principal point was solved by Schoof.

The condition $P(\mathscr{C}, b)$ non-empty, in the statement of Theorem 1, is satisfied, for example, if the order of $\mathscr{C}$ is prime to $[K:\mathbf{Q}]$ (Proposition 4(b), due to Washington) or if $K \subseteq \mathbf{Q}(\zeta_{p^r})$ and $b = p^n$ with p prime and r, n positive integers (Proposition 4(c)).

In the third section we use the results mentioned above to obtain annihilators (in $\mathbf{Z}[\Delta]$) of ideal classes of K.

Let $\mathscr{C} \in A$, b a positive integer and suppose that $P(\mathscr{C}, b)$ is non-empty. Let $Q \in P(\mathscr{C}, b)$; from (i) we get

$$\text{(iii)} \qquad \left(N_{L/K}(\alpha)\right) = \mathscr{R}_Q^b \prod_{\sigma \in \Delta} \sigma^{-1}(Q)^{r_\sigma},$$

for some ideal $\mathscr{R}_Q$ of K. If $\mathscr{R}_Q^b$ is principal, then the element $\Sigma_{\sigma \in \Delta} r_\sigma(Q)\sigma^{-1} \in \mathbf{Z}[\Delta]$ annihilates the class $\mathscr{C}$.

Suppose that $\mathscr{R}_Q^b$ is principal for each $Q \in P(\mathscr{C}, b)$; then we get a family of annihilators

$$\text{(iv)} \qquad \sum_{\sigma \in \Delta} r_\sigma(Q)\sigma^{-1}, \qquad Q \in P(\mathscr{C}, b),$$

of $\mathscr{C}$, which are related to the unit δ by Theorem 1. This apparently complicated relation between annihilators of ideal classes and units becomes simpler when we consider classes of prime power order (as we can do without loss of generality) and when we choose adequate units $\delta \in C$ to start with.

If p is a prime and p^n is an exponent of $(A)_p$, if $\mathscr{C} \in (A)_p$ and $Q \in P(\mathscr{C}, p^n)$ then, for δ and $r_\sigma(Q)$ as above, we have in (iii) that $\mathscr{R}_Q^b$ is principal with $b = p^n$ (Proposition 5). So, whenever $P(\mathscr{C}, p^n)$ is non-empty, we have a non-empty family (iv) of annihilators of $\mathscr{C}$. This condition is satisfied, for example, if $p \nmid [K: \mathbf{Q}]$, or if $K \subseteq \mathbf{Q}(\zeta_{p^r})$ for some positive integer r (by Proposition 4, (b) and (c)).

Suppose that we are in the situation above. For a convenient choice of the unit $\delta \in C$ we can get from (iv) an annihilator, of classes $\mathscr{C} \in (A)_p$, with a simpler expression. In fact, by using Theorem 1, we prove that if c_σ, $\sigma \in \Delta$, are integers, non-divisible by p, such that

$$\text{(v)} \qquad \sigma(\delta) \equiv \delta^{c_\sigma} \bmod E^{p^n},$$

then $2(\phi(|\delta|), p^n)\Sigma_{\sigma \in \Delta} c_\sigma \sigma^{-1}$ annihilates all the ideal classes $\mathscr{C}$ of $(A)_p$ such that $P(\mathscr{C}, p^n)$ is non-empty (Proposition 6).

The above result shows the importance of searching for circular units δ satisfying (v) and such that $\phi(|\delta|, p^n)$ is minimal. When $p \nmid [K: \mathbf{Q}]$ and the c_σ come from non-trivial p-adic valued Dirichlet characters χ: $\Delta \to \mathbf{Z}_p^\times$, the situation is particularly good. Let p^k be an exponent of $(W)_p$, $e_\chi \in \mathbf{Z}[\Delta]$ the idempotent corresponding to χ, and p^a the exact exponent of $e_\chi(W)_p$. We show

(Proposition 7) that there exists $\delta \in C$ such that $p^{a+1} \nmid \phi(\delta)$ and such that

$$\sigma(\delta) \equiv \delta^{\chi(\sigma)} \bmod E^{p^k}, \quad \text{for all } \sigma \in \Delta.$$

The original version of this proposition was improved and the proof simplified by Washington.

From the results cited above (Propositions 4, 6 and 7) we obtain the following (Theorem 2): If $p \nmid [K:\mathbf{Q}]$ and if χ, e_χ and p^a are as in the preceding paragraph, then p^a annihilates $e_\chi(A)_p$. As a corollary we show that when K is a real subfield of $\mathbf{Q}(\zeta_p)$, every annihilator of $(W)_p$ also annihilates $(A)_p$. When $K = \mathbf{Q}(\zeta_p + \zeta_p^{-1})$, this result can also be deduced from a theorem of Mazur and Wiles (reference [9]; see also [12], page 146).

After reading the first version of this paper, Professor Karl Rubin observed that we can also consider higher dimensional characters of Δ (with values in $\mathbf{Z}_p$) to obtain annihilators of $(A)_p$. That idea greatly strengthens the method. It allowed Washington and Rubin to obtain the beautiful result mentioned at the beginning: If $p \nmid [K:\mathbf{Q}]$ and if $\theta \in \mathbf{Z}[\Delta]$ annihilates $(W)_p$, then 2θ annihilates $(A)_p$. By a suggestion of the referees (for which I am very grateful) I include in the paper the proof of this theorem. It is done in the fourth section. Rubin also obtained recently a wide generalization of this method ([10]).

As can be seen in this introduction and in the course of the article, my debt to Lawrence Washington is enormous; his help and his lectures at the University of Maryland were indispensable to the conclusion of the first version of this paper. After that, the suggestions and the permission he gave me to use his notes, were of great help in improving both the substance and the presentation.

I am also very grateful to Professor René Schoof for his proof of the crucial point of the second section.

1. Factorization of certain principal ideals

We denote by $\mathcal{O}_F$ the ring of integers of a number field F and by (a, b) the greatest common divisor of the integers a and b. Let $K \neq \mathbf{Q}$ be a real abelian number field and ζ_m a primitive m-th root of unity, where m is the least positive integer such that $K \subseteq \mathbf{Q}(\zeta_m)$. Let E be the group of units of $\mathcal{O}_K$ and Δ the Galois group of $K/\mathbf{Q}$. For $j \geq 1$ we define

$$C_j(X) = \left\{ f(X) = \pm \prod_{i=1}^{j} \prod_{k=1}^{m-1} \left(X^i - \zeta_m^k\right)^{a_{ik}} : a_{ik} \in \mathbf{Z},\ f(X) \in K(X) \right.$$
$$\left. \text{and } f(1) \in E \right\},$$

where X is an indeterminate.

Let $C = \bigcup_{j=1}^{\infty} C_j(1)$. This is a subgroup of finite index of E that we call the group of circular units of K. Let $l \geq 1$ be fixed such that $C = C_l(1)$ (note that the ascending chain $C_1(1) \subseteq C_2(1) \subseteq \ldots$ must be stationary).

In this section q is an odd rational prime greater than l, that splits completely in K, ζ_q is a primitive q-th root of unity, $L = K(\zeta_q)$ and $N_{L/K}$ is the norm from L to K. The following fact is fundamental for this article.

PROPOSITION 1. *If* $f(X) \in C_l(X)$ *then* $N_{L/K}(f(\zeta_q)) = 1$.

Proof. We have that $f(\zeta_q) \in L$; hence $N_{L/K}(f(\zeta_q))$ is a well-defined element of K. If $f(X) = \pm\prod_{j=1}^{l}\prod_{k=1}^{m-1}(X^j - \zeta_m^k)^{a_{jk}}$ with $a_{jk} \in \mathbf{Z}$, then

$$N_{L/K}\big(f(\zeta_q)\big) = \prod_{j=1}^{l}\prod_{k=1}^{m-1} N_{\mathbf{Q}(\zeta_{mq})/\mathbf{Q}(\zeta_m)}\big(\zeta_q^j - \zeta_m^k\big)^{a_{jk}}$$

$$= \prod_{j=1}^{l}\prod_{k=1}^{m-1}\left(\frac{1-\zeta_m^{qk}}{1-\zeta_m^k}\right)^{a_{jk}} = f(1)^{\sigma_q - 1},$$

where σ_q: $\zeta_m \mapsto \zeta_m^q$ is the Frobenius map for q in the Galois group of $\mathbf{Q}(\zeta_m)/\mathbf{Q}$. Since q splits completely in K, $\sigma_q|_K$ is the identity map of K; hence $N_{L/K}(f(\zeta_q)) = f(1)^{\sigma_q - 1} = 1$, as we wanted to prove.

Let s be a primitive root modulo q and let τ be the K-automorphism of L such that $\tau(\zeta_q) = \zeta_q^s$. The Galois group of L/K is cyclic, generated by τ. From Hilbert's Theorem 90 and from Proposition 1, we conclude that if $f(X) \in C_l(X)$, then there exists $\alpha \in L^{\times}$ such that

$$\tau(\alpha) = f(\zeta_q)\alpha. \tag{1}$$

We are interested in the prime ideal factorization of the principal ideal (α).

Let Q be a prime ideal of K above q and B the only prime ideal of L above Q. Since $K \cap \mathbf{Q}(\zeta_q) = \mathbf{Q}$, every $\sigma \in \Delta$ can be extended, in a unique way, to a $\mathbf{Q}(\zeta_q)$-automorphism of L; we denote this extension also by σ and call Δ' the set of all such extensions of elements of Δ.

We have the following prime ideal decompositions:

$$q\mathcal{O}_K = \prod_{\sigma\in\Delta}\sigma(Q),$$

$$(\zeta_q - 1)\mathcal{O}_L = \prod_{\sigma\in\Delta'}\sigma(B),$$

$$Q\mathcal{O}_L = B^{q-1},$$

$$q\mathcal{O}_L = \prod_{\sigma\in\Delta'}\sigma(B)^{q-1}.$$

Let $\alpha \in L^{\times}$ satisfying (1) and let $(\alpha) = \alpha\mathcal{O}_L$. Since $f(\zeta_q)$ is a unit we have that $\tau(\alpha) = (\alpha)$, but the primes above q are the only primes that ramify in the

extension L/K; hence we can conclude from this equality that

$$(\alpha) = D \prod_{\sigma \in \Delta'} \sigma^{-1}(B)^{r_\sigma}, \tag{2}$$

where D is the lift of a (fractional) ideal of K relatively prime to q and $r_\sigma \in \mathbf{Z}$ (we shall see soon the advantage of writing $\sigma^{-1}(B)^{r_\sigma}$ instead of $\sigma(B)^{r_\sigma}$ in (2)).

We are going to determine the exponents r_σ in (2), modulo $q-1$. The following known fact will be used for that purpose.

LEMMA. *Let L be a number field, P a prime ideal of $\mathcal{O}_L$ and v the valuation corresponding to P. If $\gamma \in L$ is such that $v(\gamma) = 0$, then there exist $\lambda, \mu \in \mathcal{O}_L$, non-divisible by P, such that $\gamma = \lambda/\mu$.*

Let $\sigma \in \Delta'$ and α, r_σ be as above; let $\gamma = \alpha/(\zeta_q - 1)^{r_\sigma}$. By the above lemma, there exist $\lambda, \mu \in \mathcal{O}_L$, non-divisible by $\sigma^{-1}(B)$, such that $\gamma = \lambda/\mu$; clearly $\tau(\lambda) \equiv \lambda$ and $\tau(\mu) \equiv \mu \bmod \sigma^{-1}(B)$. Hence $\tau(\gamma) \equiv \gamma \not\equiv 0 \bmod \sigma^{-1}(B)$. On the other hand, we can conclude from (1) that $(\zeta_q^s - 1/\zeta_q - 1)^{r_\sigma}\tau(\gamma) = f(\zeta_q)\gamma$. Therefore

$$s^{r_\sigma}\gamma \equiv \left(\frac{\zeta_q^s - 1}{\zeta_q - 1}\right)^{r_\sigma} \tau(\gamma) = f(\zeta_q)\gamma \equiv f(1)\gamma \bmod \sigma^{-1}(B).$$

This implies that $s^{r_\sigma} \equiv f(1) \bmod \sigma^{-1}(B)$; hence $s^{r_\sigma} \equiv \sigma(f(1)) \bmod B$ and also $\bmod Q$, since $f(1) \in K$.

We restate these results in the following proposition.

PROPOSITION 2. *If $f(X) \in C_l(X)$, there exists $\alpha \in L^\times$ such that $\tau(\alpha) = f(\zeta_q)\alpha$. For any such element α,*

$$(\alpha) = D \prod_{\sigma \in \Delta'} \sigma^{-1}(B)^{r_\sigma},$$

where D is the lift of an ideal of K and the r_σ, $\sigma \in \Delta$, are integers such that

$$s^{r_\sigma} \equiv \sigma(f(1)) \bmod Q. \tag{3}$$

Taking norms we conclude that

$$\left(N_{L/K}(\alpha)\right) = D^{q-1} \prod_{\sigma \in \Delta} \sigma^{-1}(Q)^{r_\sigma}, \tag{4}$$

for some ideal D of K.

2. Ideal classes and units. A local-global theorem

We preserve the notation of the first section but, since we are going to consider a family of prime ideals Q of K above rational primes q, we shall introduce subindices when necessary. So, for example, $s = s_Q$ will be a primitive

root modulo q. To induce an order in K, we fix an embedding of K into $\mathbf{R}$. If $x \in K$ define $|x| = \sup\{x, -x\}$.

For each unit $\varepsilon \neq \pm 1$ of $\mathcal{O}_K$ we define the number $\phi(\varepsilon)$ as the greatest integer k such that $\varepsilon = \mu^k$ for some $\mu \in K$. We have $\phi(\sigma(\varepsilon)) = \phi(\varepsilon)$ for all $\sigma \in \Delta$.

Given an ideal class $\mathscr{C}$ of K and a positive integer b, we define $P(\mathscr{C}, b)$ as the set of all prime ideals $Q \in \mathscr{C}$ above odd rational primes $q > l$, splitting completely in K and such that $q \equiv 1 \bmod b$.

Let $\delta = f(1) \in C$ with $f(X) \in C_l(X)$, $\mathscr{C}$ an ideal class and b a positive integer be fixed. From (3) and (4) we conclude that for all $Q \in P(\mathscr{C}, b)$ there exists a non-zero ideal $\mathscr{R}_Q$ of K such that $\mathscr{R}_Q^b \prod_{\sigma \in \Delta} \sigma^{-1}(Q)^{r_\sigma(Q)}$ is a principal ideal, where the integers $r_\sigma(Q)$ satisfy

$$s_Q^{r_\sigma(Q)} \equiv \sigma(\delta) \bmod Q. \tag{5}$$

Suppose that the following agreeable situation occurs: $P(\mathscr{C}, b)$ is nonempty and $\mathscr{R}_Q^b$ is a principal ideal for all $Q \in P(\mathscr{C}, b)$. Then we get a family of annihilators of the ideal class $\mathscr{C}$, namely this formed with the elements $\sum_{\sigma \in \Delta} r_\sigma(Q)\sigma^{-1} \in \mathbf{Z}[\Delta]$ such that $Q \in P(\mathscr{C}, b)$. These elements are in turn related to the circular unit δ by (5). We will work with such situations in the third section. In this section we are going to investigate closely the relation between the integers $r_\sigma(Q)$ and the unit δ.

Suppose that $P(\mathscr{C}, b)$ is nonempty. Let $\sigma \in \Delta$ be fixed. We define the number $g = g(\delta, \mathscr{C}, b, \sigma)$ as the greatest common divisor of b and of all the $r_\sigma(Q)$ such that $Q \in P(\mathscr{C}, b)$. Observe that when $Q \in P(\mathscr{C}, b)$, the number $(r_\sigma(Q), b)$ is completely determined by (5) and does not depend on the choice of s_Q.

The following proposition is an immediate consequence of (5) and of the definition of g.

PROPOSITION 3. *Let $\delta, \mathscr{C}, b, \sigma$ be as above. Suppose that $P(\mathscr{C}, b)$ is nonempty and let $g = g(\delta, \mathscr{C}, b, \sigma)$; then for all $Q \in P(\mathscr{C}, b)$ there exists $\beta_Q \in \mathbf{Z}$ such that $\sigma(\delta) \equiv \beta_Q^g \bmod Q$.*

Our principal aim in this section is to prove the following:

THEOREM 1. *Let $\delta \in C \setminus \{\pm 1\}$, $\mathscr{C}$ an ideal class of K, b a positive integer and $\sigma \in \Delta$. Suppose that $P(\mathscr{C}, b)$ is nonempty and let $g = g(\delta, \mathscr{C}, b, \sigma)$; then:*

(i) *If b is odd, then $g = (\phi(\delta), b)$.*

(ii) *If b is even and $\sigma(\delta) > 0$, then $g = (\phi(\delta), b)$ or $g = 2(\phi(\delta), b)$.*

(iii) *If b is even and $\sigma(\delta) < 0$ (and even in cases* i *and* ii*), then g divides $(4/(2, b/g))(\phi(|\delta|), b)$ and is divisible by $(\phi(\delta), b)$.*

The deep part of this theorem is the fact that g divides $\phi(\delta)$ or $2\phi(\delta)$ or $(2/(2, b/g))\phi(\delta^2) = (4/(2, b/g))\phi(|\delta|)$ in cases (i), (ii) and (iii) respectively. This is a consequence of Proposition 3, but to show this we need a local-global theorem (Proposition 4(d)) whose proof requires more powerful methods including the Tchebotarev density theorem. Most of the ideas involved in that proof were suggested to me by Lawrence Washington. The crucial point was solved by René Schoof who obtained the following general result:

THEOREM. *Let K be a number field, L/K a finite extension. Let f be a divisor of K, and suppose there exists a generalized ideal class $\mathscr{C} \in \mathscr{I}_f/\mathscr{P}_f$ such that whenever a prime P of K is in $\mathscr{C}$ then P splits completely in L/K. Then L/K is an abelian extension. (We may restrict our attention to P of absolute degree 1 and also allow finitely many exceptional P).*

We do not give here the proof of this theorem because we really need a less general but stronger result. Slight modifications of Schoof's arguments are included in the proof of the following proposition. Part (b) is due to Washington.

PROPOSITION 4. *Let K be a real number field, $\mathscr{C}$ an ideal class of K, b a positive integer and $P(\mathscr{C}, b)$ the set of prime ideals of first degree belonging to $\mathscr{C}$ and dividing odd rational primes $q \equiv 1 \bmod b$. Fix an embedding of K into* $\mathbf{R}$.

a) *If $P(\mathscr{C}, b)$ is nonempty then it is an infinite set.*

b) *If K is abelian and the order of $\mathscr{C}$ is prime to $[K:\mathbf{Q}]$ then $P(\mathscr{C}, b)$ is nonempty.*

c) *If $K \subseteq \mathbf{Q}(\zeta_{p^r})$ and $b = p^n$ with p prime and r, n positive integers, then $P(\mathscr{C}, b)$ is nonempty.*

d) *Let γ be a positive element of $\mathcal{O}_k$ and $c > 0$ a divisor of b. Suppose that $P(\mathscr{C}, b)$ is nonempty and that for all, except possibly a finite set, prime ideals $Q \in P(\mathscr{C}, b)$ there exists $\beta_Q \in \mathcal{O}_K$ such that $\gamma \equiv \beta_Q^c \bmod Q$. Then $\gamma = \beta^c$ if c is odd and $\gamma = \beta^{c/2}$ if c is even, for some $\beta \in \mathcal{O}_K$.*

Observation. We can get $\gamma = \beta^c$ also when c is even in many situations, but it is a delicate matter (in relation to this see [1, Th. 1 of Chap. 9 and Th. 1 of Chap. 10]).

Proof. (If n is a positive integer we denote by ζ_n a primitive n-th root of unity.) Let H be the Hilbert class field of K. The ideal class group of K is isomorphic to $\mathrm{Gal}(H/K)$ via the Artin map. Let $\varphi \in \mathrm{Gal}(H/K)$ corresponding to $\mathscr{C}$. We affirm that $P(\mathscr{C}, b)$ is nonempty if and only if the restriction of φ to

$K(\zeta_b) \cap H$ is the identity map. In fact, suppose that $P(\mathscr{C}, b)$ is nonempty and let $Q \in P(\mathscr{C}, b)$; then $\varphi = F_Q$ the Frobenius map for Q (with respect to H/K). Since Q splits completely in $K(\zeta_b)$ we have that the restriction of φ to $K(\zeta_b) \cap H$ is the identity map. Conversely, let $J = K(\zeta_b) \cap H$ and suppose that $\varphi|_J = \mathrm{id}$, then we can extend φ to an automorphism φ' of $H(\zeta_b)$ such that $\varphi'(\zeta_b) = \zeta_b$. By the Tchebotarev density theorem there exist infinitely many prime ideals P of $H(\zeta_b)$, unramified over $\mathbf{Q}$, not dividing 2, such that the Frobenius map F_P for $H(\zeta_b)/K(\zeta_b)$ is φ' and such that the prime P' of $K(\zeta_b)$ below P is of absolute degree 1. For each such P, $F_P|_H = \varphi$ is the Frobenius map for $Q = P \cap \mathcal{O}_K$; hence $Q \in \mathscr{C}$ and since P' is of absolute degree 1 and unramified over $\mathbf{Q}$, we must have both that the same is true for Q and that the rational prime q below Q is congruent to 1 modulo b. Therefore $Q \in P(\mathscr{C}, b)$. So we have not only that $P(\mathscr{C}, b)$ is nonempty but that it contains infinite primes. This proves (a).

Now suppose that K is real abelian; then $J = K(\zeta_b) \cap H$ is abelian over $\mathbf{Q}$ and unramified over K. If a prime p divided $[J: K]$ but did not divide $[K: \mathbf{Q}]$, then there would be an unramified extension of $\mathbf{Q}$ of degree p, which is impossible. Therefore if the order of $\mathscr{C}$ is relatively prime to $[K: \mathbf{Q}]$ it is also relatively prime to $[J: \mathbf{Q}]$. Since the order of φ is the order of $\mathscr{C}$ we must have that $\varphi|_J = \mathrm{id}$; thus $P(\mathscr{C}, b)$ is nonempty. This proves (b).

To prove (c) observe that, when the hypotheses are verified, $K(\zeta_b) \subseteq \mathbf{Q}(\zeta_{p^{r+n}})$; hence $J = K(\zeta_b) \cap H$ is totally ramified and unramified over K; therefore $J = K$, $\varphi|_J = \mathrm{id}$, and the result follows.

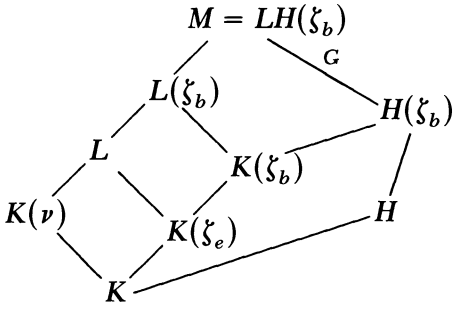
Part (d) is more difficult to prove. Let $\nu = \sqrt[c]{\gamma}$ be the positive c-th root of γ and let L be the Galois closure of $K(\nu)$ over K. Let $p(X)$ be the irreducible polynomial of ν over K; then $p(X) | X^c - \gamma$ and L is the splitting field of $p(X)$ over K. Hence $L = K(\nu, \zeta_e)$ for some $e|c$.

We are going to prove that $L \subseteq H(\zeta_b)$. Part (d) follows from this fact because then we shall have that L/K and $K(\nu)/K$ are abelian (since $H(\zeta_b)/K$ is abelian). Hence $L = K(\nu)$, $\zeta_e \in K(\nu) \subseteq \mathbf{R}$, $\zeta_e = \pm 1$, which implies that $p(X) = X - \nu$ if c is odd and $p(X) = X - \nu$ or $p(X) = X^2 - \nu^2$ if c is even. In the first case (c odd) take $\beta = \nu$; in the other case take $\beta = \nu^2$.

In order to prove that $L \subseteq H(\zeta_b)$ observe first that every $Q \in P(\mathscr{C}, b)$ not dividing γ and not belonging to the finite set of exceptions splits completely in $K(\nu)$, because the polynomial $p(X)$, reduced modulo Q, splits completely over the field $\mathcal{O}_K/Q$ (in fact: $p(X) | X^c - \gamma$, $X^c - \gamma \equiv X^c - \beta_Q^c \bmod Q$ and $\mathcal{O}_K/Q$ contains the c-th roots of unity since $c|b$ and $b|q - 1 = |(\mathcal{O}_K/Q)^\times|$) and because Q does not divide the discriminant of ν over K (reference [7]).

Hence, every $Q \in P(\mathscr{C}, b)$, not dividing γ and non-exceptional, splits completely in the Galois closure L.

Let $M = LH(\zeta_b)$ (see diagram) and, as before, let $\varphi \in \mathrm{Gal}(H/K)$ correspond to $\mathscr{C}$. By hypothesis, $P(\mathscr{C}, b)$ is nonempty; hence the restriction of φ to $K(\zeta_b) \cap H$ is the identity map. So we can extend φ to an automorphism $\tilde{\varphi}$ of M such that $\tilde{\varphi}(\zeta_b) = \zeta_b$.



Let $G = \mathrm{Gal}(M/H(\zeta_b))$ and let $f \in \tilde{\varphi}G$. By the Tchebotarev density theorem there exist infinitely many prime ideals P of M, unramified over $\mathbf{Q}$, not dividing 2, such that the prime P' of $K(\zeta_b)$ below P is of absolute degree 1 and such that the Frobenius map F_P for $M/K(\zeta_b)$ is f.

For P as above, the restriction $F_P|_H = f|_H = \varphi$ is the Frobenius map for $Q = P \cap \mathcal{O}_K$ with respect to H/K, so that $Q \in \mathscr{C}$. Since P' is of absolute degree 1, and unramified over $\mathbf{Q}$, we must have that the same is true for Q and that the rational prime q below Q is congruent to 1 modulo b. So $Q = P \cap \mathcal{O}_K \in P(\mathscr{C}, b)$ and we can choose P so as to avoid the finitely many exceptions and such that Q does not divide γ. But then Q splits completely in L, as we already showed.

Therefore $f|_L = F_P|_L = \mathrm{id}$; that is, $f \in \mathrm{Gal}(M/L)$. This proves that $\tilde{\varphi}G \subseteq \mathrm{Gal}(M/L)$, hence $\tilde{\varphi} \in \mathrm{Gal}(M/L)$ and $G \subseteq \mathrm{Gal}(M/L)$, which implies that $L \subseteq H(\zeta_b)$ as wanted.

Theorem 1 is an easy consequence of Proposition 4 and of the following lemma.

LEMMA. *Let* $\delta \in E \setminus \{\pm 1\}$. *If* $\delta = \beta^c$ *with* $\beta \in K$, *then* $c|\phi(\delta)$.

Proof. Write $\phi = \phi(\delta)$. Let $\nu \in K$ be such that $\delta = \nu^\phi$. Let $d = (c, \phi)$ and $x, y \in \mathbf{Z}$ such that $xc + y\phi = d$. Then $\delta = (\nu^x \beta^y)^{[c,\phi]}$, where $[c, \phi]$ is the least common multiple of c and ϕ. By definition of ϕ we conclude that $[c, \phi] \leq \phi$; hence $c|\phi$.

Proof of Theorem 1. Let $\delta = \mu^{\phi(\delta)}$ with $\mu \in K$. Given $Q \in P(\mathscr{C}, b)$ there exists an integer n such that $\sigma(\mu) \equiv n \bmod Q$ (since Q is of first degree). By (5)

we have $s_Q^{r_g(Q)} \equiv \sigma(\mu)^{\phi(\delta)} \equiv n^{\phi(\delta)} \bmod Q$. Hence $s_Q^{r_g(Q)} \equiv n^{\phi(\delta)} \bmod q$. This implies that $(\phi(\delta), b)$ divides $r_\sigma(Q)$, because $b|q-1$. Therefore $(\phi(\delta), b)$ divides g in any case.

By Proposition 3 we have that for all $Q \in P(\mathscr{C}, b)$, there exists $\beta_Q \in \mathbf{Z}$ such that $\sigma(\delta) \equiv \beta_Q^g \bmod Q$; hence $\sigma(\delta^2) \equiv \beta_Q^{2g} \bmod Q$. Let $c = (2g, b)$; since we are assuming $P(\mathscr{C}, b)$ nonempty, we have by Proposition 4(d) that $\sigma(\delta) = \gamma^g$ or $\sigma(\delta) = \gamma^{g/2}$ if $\sigma(\delta) > 0$ and that $\sigma(\delta^2) = \gamma'^c$ if c is odd and $\sigma(\delta^2) = \gamma'^{c/2}$ if c is even, for some $\gamma, \gamma' \in K$. By the lemma above we conclude that:

i) If b is odd then $g = c$ divides $(\phi(\delta^2), b) = (\phi(\delta), b)$. Therefore $g = (\phi(\delta), b)$.

ii) If b is even and $\sigma(\delta)$ is positive then g divides $2(\phi(\delta), b)$. Therefore $g = (\phi(\delta), b)$ or $g = 2(\phi(\delta), b)$.

iii) In all cases $c = (2g, b)$ divides $2\phi(\delta^2) = 4\phi(|\delta|)$; hence $c = g(2, b/g)$ divides $4(\phi(|\delta|), b)$.

This ends the proof of Theorem 1.

3. A relation between the ideal class group and the group of units of K

In this section we shall obtain annihilators of subgroups of the ideal class group A of K. These annihilators are related to the structure of the quotient group E/C.

Let p be a prime; we begin by obtaining annihilators of certain ideal classes in the p-Sylow subgroup $(A)_p$ of A.

Given $\delta \in C$, $\mathscr{C} \in A$ and b a positive integer, we conclude from (4) that for all $Q \in P(\mathscr{C}, b)$ there exists an ideal class $D_Q \in A$ such that

$$D_Q^b \prod_{\sigma \in \Delta} \sigma^{-1}(\mathscr{C})^{r_\sigma(Q)} = 1, \tag{6}$$

where the integers $r_\sigma(Q)$ are as in Proposition 2 and satisfy (5).

PROPOSITION 5. *Let $\delta \in C$ and let p^n be an exponent of $(A)_p$. If $\mathscr{C} \in (A)_p$, $Q \in P(\mathscr{C}, p^n)$ and if $r_\sigma = r_\sigma(Q)$, $\sigma \in \Delta$, are integers that satisfy $s^{r_\sigma} \equiv \sigma(\delta) \bmod Q$, where $s = s_Q$ is a primitive root modulo q (the rational prime below Q), then $\lambda = \lambda_Q = \sum_{\sigma \in \Delta} r_\sigma(Q)\sigma^{-1}$ annihilates $\mathscr{C}$ (i.e. $\mathscr{C}^\lambda = 1$).*

Proof. Note that the integers r_σ are uniquely determined modulo p^n, because $p^n|q-1$. Since also $\mathscr{C}^{p^n} = 1$, we have that (6) holds, with $b = p^n$. Since all conjugates of $\mathscr{C}$ belong to $(A)_p$ we conclude that $D_Q^{p^n} \in (A)_p$; hence $D_Q \in (A)_p$ and $D_Q^{p^n} = 1$. Therefore $\mathscr{C}^\lambda = 1$ (again by (6)). This ends the proof of the proposition.

Proposition 5 gives a nonempty set of annihilators of $\mathscr{C} \in (A)_p$ whenever $P(\mathscr{C}, p^n)$ is nonempty. If $p \nmid [K:\mathbf{Q}]$ or if $K \subseteq \mathbf{Q}(\zeta_{p^r})$ for some positive integer r, this condition is satisfied (by Proposition 4, (b) and (c)).

We have been working with arbitrary circular units δ. The congruences $s^{r_\sigma} \equiv \sigma(\delta) \bmod Q$ of Proposition 5, suggest that certain δ, "well-behaved" with respect to conjugation, must be specially considered in order to get a workable set of exponents r_σ. The aim is to obtain efficient annihilators of $(A)_p$.

PROPOSITION 6. *Let p^n be an exponent of $(A)_p$. Suppose that $\delta \in C$ is such that for all $\sigma \in \Delta$ there exists an integer c_σ, non-divisible by p, such that*

$$\sigma(\delta) \equiv \delta^{c_\sigma} \bmod E^{p^n}. \tag{7}$$

Let $\mathscr{C} \in (A)_p$ be such that $P(\mathscr{C}, p^n)$ is nonempty and denote the element $\sum_{\sigma \in \Delta} c_\sigma \sigma^{-1} \in \mathbf{Z}[\Delta]$ by ω; then:

i) *If p is odd, $(\phi(\delta), p^n)\omega$ annihilates $\mathscr{C}$.*

ii) *If $p = 2$, $2(\phi(|\delta|), 2^n)\omega$ annihilates $\mathscr{C}$.*

Proof. Let $Q \in P(\mathscr{C}, p^n)$ and let q, s, $r_\sigma = r_\sigma(Q)$, $\sigma \in \Delta$, be as in Proposition 5. We know, by that proposition, that $\lambda_Q = \sum_{\sigma \in \Delta} r_\sigma(Q)\sigma^{-1}$ annihilates $\mathscr{C}$. Let $d = d(Q)$ be a positive integer such that $\delta \equiv s^d \bmod Q$ (recall that Q is of first degree). Given $\sigma \in \Delta$ we have

$$s^{r_\sigma} \equiv \sigma(\delta) = \delta^{c_\sigma} \varepsilon_\sigma^{p^n} \equiv s^{dc_\sigma + p^n t} \bmod Q$$

for some $\varepsilon_\sigma \in E$ and a positive integer t such that $\varepsilon_\sigma \equiv s^t \bmod Q$. Therefore $s^{r_\sigma} \equiv s^{dc_\sigma + p^n t} \bmod q$. Since $p^n | q - 1$, this congruence implies that

$$r_\sigma(Q) \equiv d(Q)c_\sigma \bmod p^n \quad \text{for all } \sigma \in \Delta; \tag{8}$$

therefore $\lambda_Q \equiv d(Q)\sum_{\sigma \in \Delta} c_\sigma \sigma^{-1} \bmod p^n$.

Since p^n and the λ_Q, $Q \in P(\mathscr{C}, p^n)$, annihilate $\mathscr{C}$, we must have that $g_0 \sum_{\sigma \in \Delta} c_\sigma \sigma^{-1}$ annihilates $\mathscr{C}$, where g_0 is the greatest common divisor of p^n and of all the $d(Q)$ such that $Q \in P(\mathscr{C}, p^n)$. Given $\sigma \in \Delta$, since the c_σ are prime to p, we have, by (8), that g_0 is also the greatest common divisor of p^n and of the $r_\sigma(Q)$ such that $Q \in P(\mathscr{C}, p^n)$; that is $g_0 = g(\delta, \mathscr{C}, p^n, \sigma)$. Affirmation (i) is now an immediate consequence of Theorem 1, and so is affirmation (ii) when we observe that for $p = 2$, $|\delta|$ satisfies (7) when δ does.

Proposition 6 shows the convenience of searching for units $\delta \in C$, satisfying (7) and such that $(\phi(|\delta|), p^n)$ is minimal; we are going to obtain an upper bound for this minimal value.

We denote by W the quotient group E/C and by $(W)_p$ its p-Sylow subgroup. Let c_σ, $\sigma \in \Delta$, be integers non-divisible by p and

$$S = \left\{ \varepsilon \in E\colon \sigma(\varepsilon) \equiv \varepsilon^{c_\sigma} \bmod E^{p^n} \text{ for all } \sigma \in \Delta \right\}.$$

It is a subgroup of E. If p^k is an exponent of $(W)_p$, then $S/S \cap E^{p^k}C$ is isomorphic to a subgroup of $(W)_p$, because $(W)_p \simeq W/W^{p^k} \simeq E/E^{p^k}C$. Let p^a be the exact exponent of this subgroup and p^b the least of the numbers $(\phi(|\varepsilon|), p^n)$ such that $\varepsilon \in S$. Then, there exists $\delta \in C \cap S$ such that $(\phi(|\delta|), p^n)$ divides p^{a+b}. In fact, let $\varepsilon \in S$ be such that $(\phi(|\varepsilon|), p^n) = p^b$. Since $\varepsilon^{p^a} \in S \cap E^{p^k}C$, there exists t non-divisible by p such that $\delta = \varepsilon^{p^a t} \in S \cap C$, and we have that $\phi(|\delta|) = p^a t \phi(|\varepsilon|)$. The following proposition shows an important case in which $p^b = 1$.

PROPOSITION 7. *Suppose that* $p \nmid [K:\mathbf{Q}]$. *Let* p^k *be an exponent of* $(W)_p$, $\chi\colon \Delta \to \mathbf{Z}_p^\times$ *a non-trivial p-adic-valued Dirichlet character,* $e_\chi = (1/|\Delta|)\sum_{\sigma \in \Delta} \chi(\sigma)\sigma^{-1} \in \mathbf{Z}_p[\Delta]$ *the corresponding idempotent and* p^a *the exact exponent of the* χ*-component* $e_\chi(W)_p$ *of* $(W)_p$. *Then there exists* $\delta \in C$ *such that* $p^{a+1} \nmid \phi(\delta)$ *and such that*

$$\sigma(\delta) \equiv \delta^{\chi(\sigma)} \bmod E^{p^k}, \quad \textit{for all } \sigma \in \Delta. \tag{9}$$

Proof. The affirmation is trivial if $k = 0$; assume $k \geq 1$. Since $(W)_p \simeq E/E^{p^k}C$ (canonical isomorphism of $\mathbf{Z}_p[\Delta]$-modules) we have

$$e_\chi(W)_p \simeq e_\chi\left(E/E^{p^k}C\right) \simeq \frac{e_\chi\left(E/E^{p^k}\right)}{e_\chi\left(E^{p^k}C/E^{p^k}\right)};$$

so the elements $\eta \in E$ such that $\eta C \in e_\chi(W)_p$ are the same as the elements $\eta \in E$ such that $\eta E^{p^k} \in e_\chi(E/E^{p^k})$. Therefore, for such elements η, we have $\eta^{p^a c} \in C$, for some c prime to p, and

$$\sigma(\eta) \equiv \eta^{\chi(\sigma)} \bmod E^{p^k}.$$

We affirm that there exists some η as above such that $\eta \notin E^p$. In fact, otherwise we would have

$$e_\chi\left(E/E^{p^k}\right) \subseteq E^p/E^{p^k} = \left(E/E^{p^k}\right)^p,$$

which implies that

$$e_\chi\left(E/E^{p^k}\right) \subseteq e_\chi\left(E/E^{p^k}\right)^p \subseteq \cdots \subseteq e_\chi\left(E/E^{p^k}\right)^{p^k} = 1.$$

That is, $e_\chi(E/E^{p^k}) = 1$. Then, since for $j \geq k$

$$e_\chi\left(E/E^{p^k}\right) \simeq e_\chi\left(\frac{E/E^{p^j}}{\left(E/E^{p^j}\right)^{p^k}}\right) \simeq \frac{e_\chi\left(E/E^{p^j}\right)}{e_\chi\left(E/E^{p^j}\right)^{p^k}},$$

we must have that $e_\chi(E/E^{p^j}) = 1$ for all $j \geq 1$.

Let $\hat{E}$ be the inverse limit $\lim_{\leftarrow}(E/E^{p^j})$. For the above equality $e_\chi(\hat{E}) = 1$.

We affirm that there is a unit $\varepsilon \in E$ such that the subgroup $\{\varepsilon^\lambda\colon \lambda \in \mathbf{Z}_p[\Delta]\}$ of $\hat{E}$ has a finite index in this group. It is a consequence of the following:

LEMMA. *There exists $\varepsilon \in E$ such that the subgroup $\{\varepsilon^\lambda\colon \lambda \in \mathbf{Z}[\Delta]\}$ has a finite index in E.*

Proof (similar to the existence of a normal basis for normal extensions of infinite fields; see [3, Chap. V, §10, Theorems 4 and 5]). Clearly it is enough to show that

$$\det\left[\ln\left|\sigma_i\sigma_j(\varepsilon)\right|\right]_{1\leq i,\, j\leq r} \neq 0,$$

for some $\varepsilon \in E$, where $\Delta = \{\sigma_0 = \mathrm{id}, \sigma_1, \ldots, \sigma_r\}$, $r = |\Delta| - 1$. Consider the polynomial

$$f(X_1, \ldots, X_r) = \det\left[X_{p(i,\, j)}\right]_{1\leq i,\, j\leq r},$$

where the integers $p(i, j)$, $0 \leq p(i, j) \leq r$, are defined by $\sigma_i\sigma_j = \sigma_{p(i,\, j)}$ and $X_0 = -X_1 - \cdots - X_r$. Since $f(1, \ldots, 1) = \pm|\Delta|^{|\Delta|-2} \neq 0$ we have that $f \neq 0$. Let $\varepsilon_1, \ldots, \varepsilon_r$ be a fundamental system of units of K. If we had

$$f\left(\ln\left|\sigma_1(\varepsilon)\right|, \ldots, \ln\left|\sigma_r(\varepsilon)\right|\right) = 0$$

for all $\varepsilon = \varepsilon_1^{y_1} \ldots \varepsilon_r^{y_r}$, with $y_i \in \mathbf{Z}$, then the polynomial

$$g(Y_1, \ldots, Y_r) = f\left(\sum_{j=1}^{r} \ln\left|\sigma_1(\varepsilon_j)\right| Y_j, \ldots, \sum_{j=1}^{r} \ln\left|\sigma_r(\varepsilon_j)\right| Y_j\right)$$

would be identically zero (since $g(y_1, \ldots, y_n) = 0$ for all $(y_j) \in \mathbf{Z}^r$); but this is impossible because $f \neq 0$ and the matrix $[\ln|\sigma_i(\varepsilon_j)|]_{1\leq i,\, j\leq r}$ is invertible. This ends the proof of the lemma.

Now, for ε as above, consider the function $\lambda \mapsto \varepsilon^\lambda$ from $\mathbf{Z}_p[\Delta]$ to $\hat{E}$. From what we have shown, its kernel is the ideal of $\mathbf{Z}_p[\Delta]$ generated by e_{χ_0} (χ_0 the trivial character). Since this kernel contains e_χ we must have $\chi = \chi_0$, a contradiction.

Therefore there exists some $\eta \in E$ as claimed. Let c be prime to p, such that $\delta = \eta^{p^a c} \in C$; then δ satisfies the conditions of the proposition. Note that

$p^{a+1} \nmid \phi(\delta)$ since $p \nmid \phi(\eta)$ and the conditions on χ force p to be odd (the only roots of unity in $\mathbf{Z}_2$ are ± 1, $p \nmid |\Delta|$ and χ is non-trivial).

From Propositions 4, 6 and 7 we obtain the following:

THEOREM 2. *Let p be a prime such that $p \nmid [K:\mathbf{Q}]$, $\chi\colon \Delta \to \mathbf{Z}_p^{\times}$ be a non-trivial p-adic valued Dirichlet character, $e_\chi \in \mathbf{Z}_p[\Delta]$ the corresponding idempotent. If p^a is the exact exponent of $e_\chi(W)_p$, then p^a annihilates $e_\chi(A)_p$.*

Proof. As in Proposition 7, the conditions on χ force p to be odd. Let p^n be an exponent of both $(A)_p$ and $(W)_p$. For each $\sigma \in \Delta$ let c_σ be a rational integer such that $c_\sigma \equiv \chi(\sigma) \bmod p^n$. From Proposition 7 we know that there exists $\delta \in C$ such that $p^{a+1} \nmid \phi(\delta)$ and such that $\sigma(\delta) \equiv \delta^{\chi(\sigma)} \equiv \delta^{c_\sigma} \bmod E^{p^n}$ for all $\sigma \in \Delta$.

Let $\mathscr{C} \in (A)_p$; Proposition 4(b) guarantees that $P(\mathscr{C}, p^n)$ is nonempty. Therefore, by Proposition 6, we have that $(\phi(\delta), p^n)\Sigma_{\sigma\in\Delta} c_\sigma \sigma^{-1}$ annihilates $\mathscr{C}$. But $(\phi(\delta), p^n) | p^a$ (since $p^{a+1} \nmid \phi(\delta)$) and $\Sigma_{\sigma\in\Delta} c_\sigma \sigma^{-1} \equiv |\Delta| e_\chi \bmod p^n$. Since $\mathscr{C}^{p^n} = 1$ and $p \nmid |\Delta|$ we conclude that $p^a e_\chi$ annihilates $\mathscr{C}$. This proves that p^a annihilates $e_\chi(A)_p$.

COROLLARY. *Let p be an odd prime. If $K \subseteq \mathbf{Q}(\zeta_p) \cap \mathbf{R}$, then every annihilator (in $\mathbf{Z}[\Delta]$) of $(W)_p$ also annihilates $(A)_p$.*

Proof. Let $\Sigma_{\sigma\in\Delta} b_\sigma \sigma \in \mathbf{Z}[\Delta]$ be an annihilator of $(W)_p$. Let χ be a non-trivial p-adic-valued Dirichlet character of Δ. Since $(\Sigma_{\sigma\in\Delta} b_\sigma \sigma) e_\chi = \Sigma_{\sigma\in\Delta} b_\sigma \chi(\sigma) e_\chi$, we have that $\Sigma_{\sigma\in\Delta} b_\sigma \chi(\sigma)$ annihilates $e_\chi(W)_p$. Let $p^{a(\chi)}$ be the exact exponent of this group; then

$$\sum_{\sigma\in\Delta} b_\sigma \chi(\sigma) \equiv 0 \bmod p^{a(\chi)}. \tag{10}$$

Since $K \subseteq \mathbf{Q}(\zeta_p)$, we have that $\Sigma_\chi e_\chi = 1$, where χ runs over all p-adic-valued Dirichlet characters of Δ. Therefore

$$\sum_{\sigma\in\Delta} b_\sigma \sigma = \sum_{\sigma\in\Delta} b_\sigma \sigma \sum_\chi e_\chi = \sum_\chi \sum_{\sigma\in\Delta} b_\sigma \chi(\sigma) e_\chi.$$

By (10) and by Theorem 2, $\Sigma_{\sigma\in\Delta} b_\sigma \chi(\sigma) e_\chi$ annihilates $(A)_p$ for all χ; therefore $\Sigma_{\sigma\in\Delta} b_\sigma \sigma$ also does. This ends the proof of the corollary.

4. Annihilators of ideal classes of order prime to $[K:\mathbf{Q}]$

This section is an adaptation of L. Washington's notes. Here we give an exposition of K. Rubin's idea of using higher dimensional characters to extend

the results above (Theorem 2). The result we want to prove is the following:

THEOREM 3. *With the notation above, suppose that* $p \nmid [K:\mathbf{Q}]$ *and that* $\theta \in \mathbf{Z}[\Delta]$ *annihilates* $(W)_p$; *then* 2θ *annihilates* $(A)_p$.

We need some preparation before proving this theorem. To simplify notation, we identify, several times in what follows, elements of a given abelian group with its class modulo a subgroup.

Suppose that $p \nmid [K:\mathbf{Q}]$ and let $p^n > 4$ be an exponent of both $(A)_p$ and $(W)_p$. Let $\mathscr{C} \in (A)_p$. By Proposition 4(b) we know that $P(\mathscr{C}, p^n)$ is nonempty.

For each $Q \in P(\mathscr{C}, p^n)$ choose a primitive root s modulo q (the rational prime below Q) and define a function

$$\varphi_Q\colon C/C \cap E^{p^n} \to \frac{\mathbf{Z}}{p^n\mathbf{Z}}[\Delta] \quad \text{by}$$

$$\varphi_Q\colon \delta \mapsto \sum_{\sigma\in\Delta} r_\sigma \sigma^{-1},$$

where the $r_\sigma = r_\sigma(Q)$ are integers (uniquely determined modulo p^n) such that $s^{r_\sigma} \equiv \sigma(\delta) \bmod Q$. It is easy to check that the φ_Q are well-defined homomorphisms of $\mathbf{Z}_p[\Delta]$-modules. Also, by Proposition 5, we have that $\mathscr{C}^{\varphi_Q(\delta)} = 1$ for all $\delta \in C/C \cap E^{p^n}$.

Since $p \nmid |\Delta|$, we may decompose (via Maschke's theorem)

$$\mathbf{F}_p[\Delta] = \bigoplus_\rho e_\rho \mathbf{F}_p[\Delta],$$

where ρ runs through the irreducible (over $\mathbf{F}_p$) characters of Δ with values in $\mathbf{F}_p$. There is a corresponding decomposition (see [4], Theorem 6.8)

$$\mathbf{Z}_p[\Delta] = \bigoplus_\rho e_\rho \mathbf{Z}_p[\Delta]$$

(by abuse of notation we use e_ρ to denote both the p-adic and $\mathbf{F}_p$ idempotent).

Let ρ be any non-trivial irreducible character of Δ with values in $\mathbf{F}_p$; since the φ_Q are $\mathbf{Z}_p[\Delta]$-module homomorphisms, we have the restriction

$$\varphi_Q^\rho\colon e_\rho\big(C/C \cap E^{p^n}\big) \to e_\rho \frac{\mathbf{Z}}{p^n\mathbf{Z}}[\Delta].$$

Let $p^a = p^{a_\rho}$ be the exact exponent of $e_\rho(W)_p$. There exists $\delta \in e_\rho(C/C \cap E^{p^n})$ such that $p^{a+1} \nmid \phi(|\delta|)$. The proof of Proposition 7 works as well in this general situation. Observe that if $p = 2$ then (with the notation of that proof) $\eta \notin E^2$ and also $-\eta \notin E^2$; otherwise we would have for some $\varepsilon \in E$ that

$$\eta E^{2^n} = \big(\eta E^{2^n}\big)^{e_\rho} = \big(-\eta E^{2^n}\big)^{e_\rho} = \big(\varepsilon^2 E^{2^n}\big)^{e_\rho},$$

which implies that $\eta \in E^2$, a contradiction. Here we used the fact that $(-1)^{e_\rho} = 1$, when ρ is irreducible, non-trivial and $p = 2$.

For such δ, it follows from Theorem 1 that $g(\delta, \mathscr{C}, p^n, \mathrm{id})$ divides $2p^a$. Hence, there exists $Q \in P(\mathscr{C}, p^n)$ such that

$$\varphi_Q^\rho(\delta) \not\equiv 0 \bmod p^{a+1}, \quad \text{if } p \text{ is odd and}$$

$$\varphi_Q^\rho(\delta) \not\equiv 0 \bmod 2^{a+2}, \quad \text{if } p = 2.$$

For Q as above let a' be minimal such that $\varphi_Q^\rho(\delta) \not\equiv 0 \bmod p^{a'+1}$, so that $a' \leq a$ if p is odd and $a' \leq a + 1$ if $p = 2$. Then $p^{-a'}\varphi_Q^\rho(\delta)$ is non-zero in $e_\rho \mathbf{F}_p[\Delta]$. Since this is irreducible, any non-zero element generates it as an $\mathbf{F}_p[\Delta]$-module, so that

$$p^{-a'}\varphi_Q^\rho(\delta)\mathbf{F}_p[\Delta] = e_\rho \mathbf{F}_p[\Delta].$$

Now, $\mathbf{Z}/p^n\mathbf{Z}$ is a local ring with maximal ideal $p\mathbf{Z}/p^n\mathbf{Z}$ and residue field $\mathbf{F}_p$. The $\mathbf{Z}/p^n\mathbf{Z}$-module $e_\rho(\mathbf{Z}/p^n\mathbf{Z})[\Delta]$ has the elements $p^{-a'}\varphi_Q^\rho(\delta)\sigma$, $\sigma \in \Delta$, whose images in $e_\rho \mathbf{F}_p[\Delta]$ form, by the above equality, a basis of this $\mathbf{F}_p$-vector space. Hence, by an application of Nakayama's lemma (see [2], Proposition 2.8) we have that these elements generate $e_\rho(\mathbf{Z}/p^n\mathbf{Z})[\Delta]$; that is

$$p^{-a'}\varphi_Q^\rho(\delta)\frac{\mathbf{Z}}{p^n\mathbf{Z}}[\Delta] = e_\rho \frac{\mathbf{Z}}{p^n\mathbf{Z}}[\Delta].$$

This implies that

$$\mathrm{Image}(\varphi_Q^\rho) \supseteq p^{a'}e_\rho \frac{\mathbf{Z}}{p^n\mathbf{Z}}[\Delta] \supseteq 2p^a e_\rho \frac{\mathbf{Z}}{p^n\mathbf{Z}}[\Delta].$$

Therefore we have that $2p^a e_\rho$ annihilates $\mathscr{C}$. Since $\mathscr{C} \in (A)_p$ is arbitrary, we have proved that $2p^{a_\rho}e_\rho$ annihilates $(A)_p$ (of course we may now allow ρ = trivial character).

We can now prove Theorem 3. Let $\theta \in \mathbf{Z}_p[\Delta]$ be an annihilator of $(W)_p$; then for any character ρ as above, we have that θe_ρ annihilates $e_\rho(W)_p$. Let p^b be the maximal power of p dividing θe_ρ. As above, we find that $\theta e_\rho(\mathbf{Z}/p^n\mathbf{Z})[\Delta] = p^b e_\rho(\mathbf{Z}/p^n\mathbf{Z})[\Delta]$. In particular there exists θ' such that $\theta e_\rho \theta' = p^b e_\rho$. Therefore p^b annihilates $e_\rho(W)_p$, so that $b \geq a_\rho$. This proves that $p^{a_\rho} | \theta e_\rho$; hence $2\theta e_\rho$ annihilates $(A)_p$. Finally, since 2θ is the sum, over the irreducible ρ, of $2\theta e_\rho$ we have that 2θ annihilates $(A)_p$.

UNIVERSIDADE ESTADUAL DE CAMPINAS, CAMPINAS, SP., BRAZIL

REFERENCES

[1] E. ARTIN and J. TATE, *Class Field Theory*, Benjamin, New York (1967).
[2] M. F. ATIYAH and I. G. MACDONALD, *Introduction to Commutative Algebra*, Addison-Wesley, Reading, MA (1969).
[3] N. BOURBAKI, *Algèbre*, Hermann, Paris (1967).

[4] C. Curtis and I. Reiner, Methods of representation theory, *Pure and Applied Mathematics*, John Wiley & Sons, Inc., New York (1981).
[5] E. Kummer, Über eine besondere Art, aus complexen Einheiten gebildeter Ausdrücke, J. reine angew. Math. **50** (1855), 212–232.
[6] S. Lang, *Algebra*, Addison-Wesley, Reading, MA (1965).
[7] _____, *Algebraic Number Theory*, Addison-Wesley, Reading, MA (1970).
[8] _____, *Cyclotomic Fields*, Graduate Texts in Mathematics, Springer-Verlag, New York (1978).
[9] B. Mazur and A. Wiles, Class fields of abelian extensions of **Q**, Invent. Math. **76** (1984), 179–330.
[10] K. Rubin, Global units and ideal class groups, to appear in Invent. Math.
[11] W. Sinnott, On the Stickelberger ideal and the circular units of an abelian field, Invent. Math. **62** (1980), 181–234.
[12] L. C. Washington, *Introduction to Cyclotomic Fields*, Graduate Texts in Mathematics, Springer-Verlag, New York (1982).

(Received July 9, 1986)